A New M-ary Sequence Family Constructed from Sidel'nikov Sequences

Jung-Soo Chung, Jong-Seon No
Department of EECS, INMC,
Seoul National University,
Seoul 151-744, Korea
Email: integer@ccl.snu.ac.kr, jsno@snu.ac.kr

Habong Chung
School of Electronics and Electrical Engineering,
Hongik University,
Seoul 121-791, Korea
Email: habchung@hongik.ac.kr

***Abstract*—In this paper, a new family of M-ary sequences of period p^n-1 is proposed, which has large family size and the good correlation property, that is, the maximum magnitude of their correlation values is upper bounded by $4\sqrt{p^n}+5$.**

***Index Terms*—correlation, M-ary sequences, Sidel'nikov sequences**

I. Introduction

For positive integers n and M and a prime p such that $M|p^n-1$, Sidel'nikov [1] constructed M-ary sequences, called *Sidel'nikov sequences* of period p^n-1, the out-of-phase autocorrelation magnitude of which is upper bounded by 4.

Krone and Sarwate [2] proposed the families of quaternary Sidel'nikov sequences of length $q-1$ which have their maximum magnitude of correlation values upper bounded by $3\sqrt{q}+5$ and the size of the family is $2(q+1)$ for the finite field F_q. Kim, Chung, No, and Chung [3] constructed a family of M-ary Sidel'nikov sequences with period p^n-1 such that $M|p^n-1$, whose maximum magnitude of correlation values is upper bounded by $3\sqrt{p^n}+5$. The size of this sequence family is $(M-1)^2(\frac{p^n-3}{2})+\frac{M(M-1)}{2}$ for an odd prime p. When $M=4$, the size of this family is more than twice bigger than the family in [2] while keeping the maximum correlation magnitude the same. Han and Yang [4] constructed the construction for M-ary sequence families using the shift and addition of power residue sequences, whose correlation magnitudes are bounded by $2\sqrt{p^n}+6$, where p^n-1 is the period N. The size of this sequence family is $\frac{(M-1)}{2}N+\lfloor\frac{M-1}{2}\rfloor$, where $\lfloor a\rfloor$ denotes the largest integer less than or equal to a.

In this paper, a new family of M-ary sequences of period p^n-1 is proposed. This family whose maximum correlation magnitude is upper bounded by $4\sqrt{p^n}+5$ contains roughly twice as many sequences as the one in [3].

II. Preliminaries

For an M-ary sequences $s_i(t)$ and $s_j(t)$ of period N, the correlation function $R_{s_i,s_j}(\tau)$ is defined as

$$R_{s_i,s_j}(\tau)=\sum_{t=0}^{N-1}\omega_M^{s_i(t)-s_j(t+\tau)},\qquad 0\le\tau\le N-1$$

where $\omega_M=e^{j2\pi/M}$.

Definition 1 ([5]): Let p be a prime and α a primitive element in the finite field F_{p^n} with p^n elements. Let M be a positive integer such that $M\ge 2$ and $M|p^n-1$. Let S_k, $k=0,1,\cdots,M-1$, be the disjoint subsets of F_{p^n} defined by

$$S_k=\left\{\alpha^{Mi+k}-1 \mid 0\le i<\frac{p^n-1}{M}\right\}.$$

An M-ary Sidel'nikov sequence $s(t)$ of period p^n-1 is defined as

$$s(t)=\begin{cases}k, & \text{if } \alpha^t\in S_k,\ 0\le k\le M-1\\ k_0, & \text{if } \alpha^t=-1\end{cases}\tag{1}$$

where k_0 is some integer modulo M. ■

It is known that the M-ary Sidel'nikov sequence $s(t)$ in (1) can be represented in terms of the multiplicative character $\psi_M(\cdot)$ of order M in F_{p^n} and the indicator function $I(\cdot)$ as

$$\omega_M^{s(t)}=\omega_M^{k_0}I(\alpha^t+1)+\psi_M(\alpha^t+1)\tag{2}$$

where $I(x)=1$ if $x=0$ and otherwise, $I(x)=0$ and the multiplicative character ψ_M is defined as $\psi_M(\alpha^t)=e^{j2\pi t/M}$ and $\psi_M(0)=0$.

Knowing the cross-correlation between Sidel'nikov sequences has the utmost importance if one wants to design a family of Sidel'nikov sequences with low correlation. The evaluation of the correlation values between Sidel'nikov sequences may require the value of a summation of products of multiplicative characters over the given finite field. The following theorem provides us an upper bound on a sum of products of multiplicative characters.

Theorem 2 ([6]): Let $f_1(z),f_2(z),\cdots,f_l(z)$ be l monic pairwisely prime polynomials in $F_{p^n}[z]$ whose highest-degree squarefree divisors have degrees $h_1,h_2,\cdots,h_l$. Let $\chi_1,\chi_2,\cdots,\chi_l$ be non-trivial multiplicative characters of F_{p^n}. Assume that for any $1\le i\le l$, the polynomial $f_i(z)$ is not of the form $g(z)^{ord(\chi_i)}$ in $F_{p^n}[z]$, where $ord(\chi)$ is the smallest positive integer h such that $\chi^h=1$ and $g(z)$ is a polynomial in $F_{p^n}[z]$. Then, we have

$$\left|\sum_{z\in F_{p^n}}\chi_1(f_1(z))\chi_2(f_2(z))\cdots\chi_l(f_l(z))\right|\le(\sum_{i=1}^{l}h_i-1)p^{n/2}.$$

■

978–1–4244–6014–4/10/$26.00 © 2010 IEEE

III. Constructions of the Families of M-ary Sequences

Kim, Chung, No, and Chung [3] proposed the families of M-ary sequences and derived the family size and the upper bound on the maximum magnitude of correlation values.

Theorem 3 ([3]): Let $s(t)$ be an M-ary Sidel'nikov sequence of period p^n-1 defined in (1) and (2). Let $T = \lceil \frac{p^n-1}{2} \rceil$, where $\lceil a \rceil$ denotes the least integer larger than or equal to a. The family $\mathcal{L}$ is defined as

i) For $p=2$;

$$\begin{aligned}\mathcal{L} =&\{u_{0,c_1}(t) \mid 1 \le c_1 \le M-1\}\\ &\cup \{u_{i,c_1,c_2}(t) \;\Big|\; 1 \le c_1, c_2 \le M-1, 1 \le i \le T-1\}.\end{aligned}$$

ii) For an odd prime p;

$$\begin{aligned}\mathcal{L} =&\{u_{0,c_1}(t) \mid 1 \le c_1 \le M-1\}\\ &\cup \{u_{i,c_1,c_2}(t) \;\Big|\; 1 \le c_1, c_2 \le M-1, 1 \le i \le T-1\}\\ &\cup \{u_{T,c_1,c_2}(t) \;\Big|\; 1 \le c_1 < c_2 \le M-1\}\end{aligned}$$

where $u_{0,c_1}(t) = c_1 s(t)$ and $u_{i,c_1,c_2}(t) = c_1 s(t) + c_2 s(t+i)$. The family size of $\mathcal{L}$ is $(M-1)^2(T-1)+(M-1)$ for $p=2$ or $(M-1)^2(T-1)+M(M-1)/2$ for an odd prime p. The magnitude of the correlation values of any two M-ary sequences in the family $\mathcal{L}$ is upper bounded by

$$|R(\tau)| \le 3\sqrt{p^n}+5. \qquad \blacksquare$$

We can slightly modify the construction in Theorem 3 by introducing the reverse sequence $s(-t)$ to get a new family $\mathcal{K}$ as in the following theorem.

Theorem 4: Let $s(t)$ be an M-ary Sidel'nikov sequence of period p^n-1. Let $T = \lceil \frac{p^n-1}{2} \rceil$. Let $\mathcal{K}$ be the set of M-ary sequences of period p^n-1 given as:

1) For $p=2$;

$$\begin{aligned}\mathcal{K} =&\{v_{0,a_1}(t) \mid 1 \le a_1 \le M-1\}\\ &\cup \{v_{i,a_1,a_2}(t) \;\Big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\}\\ &\cup \{v_{1,a_1}(t) \mid 1 \le a_1 \le M-1\}. \qquad (3)\end{aligned}$$

2) For an odd prime p;

$$\begin{aligned}\mathcal{K} =&\{v_{0,a_1}(t) \mid 1 \le a_1 \le M-1\}\\ &\cup \{v_{1,a_1}(t) \mid 1 \le a_1 \le M-1\}\\ &\cup \{v_{i,a_1,a_2}(t) \;\Big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\}\\ &\cup \{v_{T,a_1,a_2}(t) \;\Big|\; 1 \le a_1, a_2 \le M-1, a_1 \ne a_2\} \qquad (4)\end{aligned}$$

where $v_{0,a_1}(t) = a_1 s(t)$, $v_{1,a_1}(t) = a_1 s(-t)$, and $v_{i,a_1,a_2}(t) = a_1 s(t) + a_2 s(-t+i)$.

The magnitude of the correlation values of any two M-ary sequences in the family $\mathcal{K}$ except for the case of $p=2, n=4$, and $M=5$ is upper bounded by

$$|R(\tau)| \le 4\sqrt{p^n}+5$$

and the family size is $(M-1)^2(T-1)+2(M-1)$ for $p=2$ and $(M-1)^2(T-1)+M(M-1)$ for an odd prime p.

Proof: The reason why i is less than T is because the magnitude of the cross-correlation value of $v_{i,a_1,a_2}(t)$ and $v_{N-i,a_1,a_2}(t)$ is almost the same as N. Similarly, we have to remove $v_{T,a_1,a_1}(t) = a_1 s(t) + a_1 s(-t+T)$ in $\mathcal{K}$ because the magnitude of the autocorrelation value of $v_{T,a_1,a_1}(t)$ is almost the same as N. Differently from $\mathcal{L}$ of Theorem 3, the condition $a_1 < a_2$ in $\mathcal{K}$ can be replaced with $a_1 \ne a_2$.

We will prove the theorem for the odd prime p. The case of $p=2$ can be done similarly.

Case 1) Correlation between $v_{i,a_1,a_2}(t)$ and $v_{j,a_3,a_4}(t)$;

The cross-correlation of two sequences $v_{i,a_1,a_2}(t)$ and $v_{j,a_3,a_4}(t)$ can be written as

$$\begin{aligned}R_{v_{i,a_1,a_2},v_{j,a_3,a_4}}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i,a_1,a_2}(t+\tau)-v_{j,a_3,a_4}(t)}\\ &= \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \psi_M^{-a_3}(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \psi_M^{-a_3}(\alpha^t+1)\omega^{-a_4 k_0} I(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \omega^{-a_3 k_0} I(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\omega^{a_2 k_0} I(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \psi_M^{-a_3}(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\omega^{a_2 k_0} I(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \psi_M^{-a_3}(\alpha^t+1)\omega^{-a_4 k_0} I(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\omega^{a_2 k_0} I(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \omega^{-a_3 k_0} I(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \omega^{a_1 k_0} I(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \psi_M^{-a_3}(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \omega^{a_1 k_0} I(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \psi_M^{-a_3}(\alpha^t+1)\omega^{-a_4 k_0} I(\alpha^{-t+j}+1)\\ &+ \sum_{t=0}^{N-1} \omega^{a_1 k_0} I(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\qquad \times \omega^{-a_3 k_0} I(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1).\end{aligned}$$

As one can see from the equation just above, $R_{v_{i,a_1,a_2},v_{j,a_3,a_4}}(\tau)$ is expressed as the sum of nine summations, which will be denoted by A_1 through A_9.

The first summation is given as

$$\begin{aligned}A_1 &= \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1) \\ &\qquad \times \psi_M^{-a_3}(\alpha^{t}+1)\psi_M^{-a_4}(\alpha^{-t+j}+1) \\ &= \sum_{z\in F_{p^n}} \psi_M^{a_1}(\alpha^{\tau}z+1)\psi_M^{a_2}(\alpha^{i-\tau}+z) \\ &\qquad \times \psi_M^{-a_3}(z+1)\psi_M^{-a_4}(\alpha^{j}+z)\psi_M^{-a_2+a_4}(z) - 1.\end{aligned}$$

From Theorem 2, all arguments of $\psi_M(\cdot)$ have the highest-degree squarefree divisor, that is, $h_1 = h_2 = h_3 = h_4 = h_5 = 1$ and thus it is easy to check $|A_1| \le 4\sqrt{p^n}+1$.

In the second summation, $I(\alpha^{-t+j}+1) = 1$ only when $t = N/2 + j$ and thus we have

$$A_2 = \begin{cases} 0, & \text{if } \tau = i-j \\ & \text{or } \tau = -j \\ \omega^{-a_4k_0}\psi_M^{a_1}(-\alpha^{j+\tau}+1) & \\ \times\psi_M^{a_2}(-\alpha^{-j-\tau+i}+1)\psi_M^{-a_3}(-\alpha^{j}+1), & \text{otherwise.}\end{cases}$$

Similarly, we have A_i as follows.

$$A_3 = \begin{cases} 0, & \text{if } \tau = 0 \\ & \text{or } \tau = i \\ \omega^{-a_3k_0}\psi_M^{a_1}(-\alpha^{\tau}+1)\psi_M^{a_2}(-\alpha^{-\tau+i}+1) & \\ \quad\times\psi_M^{-a_4}(-\alpha^{j}+1), & \text{otherwise.}\end{cases}$$

$$A_4 = \begin{cases} 0, & \text{if } \tau = i-j \\ & \text{or } \tau = i \\ \omega^{a_2k_0}\psi_M^{a_1}(-\alpha^{i}+1)\psi_M^{-a_3}(-\alpha^{-\tau+i}+1) & \\ \quad\times\psi_M^{-a_4}(-\alpha^{\tau-i+j}+1), & \text{otherwise.}\end{cases}$$

$$A_5 = \begin{cases} \omega^{(a_2-a_4)k_0}\psi_M^{a_1}(-\alpha^{i}+1)\psi_M^{-a_3}(-\alpha^{j}+1), & \text{if } \tau = i-j \\ 0, & \text{otherwise.}\end{cases}$$

$$A_6 = \begin{cases} \omega^{(a_2-a_3)k_0}\psi_M^{a_1}(-\alpha^{i}+1)\psi_M^{-a_4}(-\alpha^{j}+1), & \text{if } \tau = i \\ 0, & \text{otherwise.}\end{cases}$$

$$A_7 = \begin{cases} 0, & \text{if } \tau = 0 \\ & \text{or } \tau = -j \\ \omega^{a_1k_0}\psi_M^{a_2}(-\alpha^{i}+1)\psi_M^{-a_3}(-\alpha^{-\tau}+1) & \\ \quad\times\psi_M^{-a_4}(-\alpha^{\tau+j}+1), & \text{otherwise.}\end{cases}$$

$$A_8 = \begin{cases} \omega^{(a_1-a_4)k_0}\psi_M^{a_2}(-\alpha^{i}+1)\psi_M^{-a_3}(-\alpha^{j}+1), & \text{if } \tau = -j \\ 0, & \text{otherwise.}\end{cases}$$

$$A_9 = \begin{cases} \omega^{(a_1-a_3)k_0}\psi_M^{a_2}(-\alpha^{i}+1)\psi_M^{-a_4}(-\alpha^{j}+1), & \text{if } \tau = 0 \\ 0, & \text{otherwise.}\end{cases}$$

By summing all nine summations,we have

$$|R(\tau)| = \begin{cases} |A_1+A_2+A_4+A_9| \le 4\sqrt{p^n}+4, & \text{if } \tau = 0 \\ |A_1+A_3+A_4+A_8| \le 4\sqrt{p^n}+4, & \text{if } \tau = -j \\ |A_1+A_2+A_6+A_7| \le 4\sqrt{p^n}+4, & \text{if } \tau = i \\ |A_1+A_3+A_5+A_7| \le 4\sqrt{p^n}+4, & \text{if } \tau = i-j \\ |A_1+A_2+A_3+A_4+A_7| \le 4\sqrt{p^n}+5, & \text{otherwise.}\end{cases}$$

Thus, we prove that the cross-correlation magnitude of two sequences $v_{i,a_1,a_2}(t)$ and $v_{j,a_3,a_4}(t)$ is less than or equal to $4\sqrt{p^n}+5$.

Case 2) Correlation between $v_{1,a_1}(t)$ and $v_{j,a_3,a_4}(t)$;

Case 3) Correlation between $v_{T,a_1,a_2}(t)$ and $v_{j,a_3,a_4}(t)$;

Case 4) Correlation between $v_{0,a_1}(t)$ and $v_{1,a_2}(t)$;

Similarly to Case 1), it can be proved that the cross-correlation magnitude of two sequences for Cases 2), 3), and 4) is less than or equal to $4\sqrt{p^n}+5$.

Therefore, we prove the upper bound of the maximum correlation values for the family $\mathcal{K}$. The family size is easy to derive from (3) and (4). The family size is $(M-1)^2(T-1)+2(M-1)$ for $p=2$ and $(M-1)^2(T-1)+M(M-1)$ for an odd prime p. ∎

Certainly the upper bound on the correlation magnitude must be less than the sequence period. Therefore, we note that the period of Theorem 4 holds for the period such that $p^n \ge 4\sqrt{p^n}+5$.

Example 5: For $M=4$, $p=3$, and $n=6$, we can construct a family of quaternary sequences of period $N=728$. Let $s(t)$ be a quaternary Sidel'nikov sequence. Then the family $\mathcal{K}$ contains 3279 quaternary sequences as

$$\begin{aligned}\mathcal{K} =& \{s(t), 2s(t), 3s(t), s(-t), 2s(-t), 3s(-t)\} \\ &\cup \{a_1s(t)+a_2s(-t+i) | 1\le a_1,a_2\le 3, 1\le i\le 363\} \\ &\cup \{a_1s(t)+a_2s(-t+364) | 1\le a_1,a_2\le 3, a_1\ne a_2\}\end{aligned}$$

where the magnitude of their correlation values is upper bounded by 112.

To generalize Theorems 3 and 4, we must check correlation between $s(t)+s(dt+i)$ and $s(t+\tau)+s(dt+d\tau+i)$, where $\gcd(d,p^n-1)=1$. Similarly to A_1 of the proof of Theorem 4, we have

$$\begin{aligned}\tilde{A}_1 &= \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{dt+d\tau+i}+1) \\ &\qquad \times \psi_M^{-a_3}(\alpha^{t}+1)\psi_M^{-a_4}(\alpha^{dt+j}+1) \\ &= \sum_{z\in F_{p^n}} \psi_M^{a_1}(\alpha^{\tau}z+1)\psi_M^{a_2}(\alpha^{d\tau+i}z^d+1) \\ &\qquad \times \psi_M^{-a_3}(z+1)\psi_M^{-a_4}(\alpha^{j}z^d+1) - 1.\end{aligned}$$

If $d \ne 1$ or -1, the highest-degree squarefree divisor is larger than equal to 1 and the upper bound of correlation by Theorem 2 increases. Therefore, we only consider two cases, $d=1$ and -1.

IV. Main Construction

Certainly the family $\mathcal{K}$ itself has no merit compared to the family $\mathcal{L}$ since their sizes are almost the same but the maximum correlation magnitude is deteriorated from $3\sqrt{p^n}+5$

to $4\sqrt{p^n}+5$. But combining $\mathcal{K}$ and $\mathcal{L}$ can give us a larger family as in the following theorem. Then we have the following theorem regarding the upper bound on the correlation values for the M-ary sequence families.

Theorem 6: Let $\mathcal{M}$ be the set of M-ary sequences of period p^n-1 given as.

1) For $p=2$;

$$\begin{aligned}\mathcal{M} = &\{v_{0,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ &\cup \{v_{1,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ &\cup \{v_{i,a_1,a_2}(t) \;\big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\} \\ &\cup \{u_{i,a_1,a_2}(t) \;\big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\}.\end{aligned}$$

2) For an odd prime p;

$$\begin{aligned}\mathcal{M} = &\{v_{0,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ &\cup \{v_{1,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ &\cup \{v_{i,a_1,a_2}(t) \;\big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\} \\ &\cup \{v_{T,a_1,a_2}(t) \;\big|\; 1 \le a_1, a_2 \le M-1, a_1 \ne a_2\} \\ &\cup \{u_{i,a_1,a_2}(t) \;\big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\} \\ &\cup \{u_{T,a_1,a_2}(t) \;\big|\; 1 \le a_1 < a_2 \le M-1\}\end{aligned}$$

where $v_{0,a_1}(t) = a_1 s(t)$, $v_{i,a_1,a_2}(t) = a_1 s(t) + a_2 s(-t+i)$ $v_{1,a_1}(t) = a_1 s(-t)$, and $u_{i,a_1,a_2}(t) = a_1 s(t) + a_2 s(t+i)$. The magnitude of the correlation values of any two M-ary sequences in the large family $\mathcal{M}$ is upper bounded by

$$|R(\tau)| \le 4\sqrt{p^n} + 5.$$

The family size of $\mathcal{M}$ is $2(M-1)^2(T-1)+2(M-1)$ for $p=2$ or $2(M-1)^2(T-1)+2(M-1)+3(M-1)(M-2)/2$ for an odd prime p.

Proof: We will prove for the case of an odd prime p. The proof for $p=2$ can be done in a similar manner. First, the cross-correlation of $u_{i,a_1,a_2}(t)$ and $v_{j,a_3,a_4}(t)$ is derived for $i \ne 0$ and $j \ne 0$. Similarly to the proof of Theorem 4, we also have nine summations B_i.

Therefore, we have

$$|R(\tau)| = \begin{cases} |B_1+B_2+B_4+B_9| \le 4\sqrt{p^n}+4, & \text{if } \tau = 0 \\ |B_1+B_3+B_4+B_8| \le 4\sqrt{p^n}+4, & \text{if } \tau = -j \\ |B_1+B_2+B_6+B_7| \le 4\sqrt{p^n}+4, & \text{if } \tau = i \\ |B_1+B_3+B_5+B_7| \le 4\sqrt{p^n}+4, & \text{if } \tau = i-j \\ |B_1+B_2+B_3+B_4+B_7| \le 4\sqrt{p^n}+5, & \text{otherwise.} \end{cases}$$

Thus, we prove that the cross-correlation magnitude of two sequences $u_{i,a_1,a_2}(t)$ and $v_{j,a_3,a_4}(t)$ is less than or equal to $4\sqrt{p^n}+5$.

The remaining cross-correlation values of the sequence can be proved similarly. ∎

Note that with a little sacrifice in maximum correlation magnitude from $3\sqrt{p^n}+5$ to $4\sqrt{p^n}+5$, the family size $|\mathcal{M}|$ is almost double of $|\mathcal{L}|$.

V. Conclusion

In this paper, we proposed that a new family of M-ary sequences with period p^n-1 whose maximum correlation magnitude is upper bounded by $4\sqrt{p^n}+5$.

Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 2009-0081441) and the IT R&D program of MKE/KEIT. [2008-F-007-02, Intelligent Wireless Communication Systems in 3 Dimensional Environment]

References

[1] V. M. Sidel'nikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 1, pp. 12–16, 1969.

[2] S. M. Krone and D. V. Sarwate, "Quadriphase sequences for spread-spectrum multiple-access communication," *IEEE Trans. Inf. Theory*, vol. 30, no. 4, pp. 520–529, May 1984.

[3] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "New families of M-ary sequences with low correlation constructed from Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768–3774, Aug. 2008.

[4] Y.-K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1815–1823, Apr. 2009.

[5] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3303–3307, Sep. 2005.

[6] D. Wan, "Generators and irreducible polynomials over finite fields," *Mathematics of Computations*, vol. 66, no. 219, pp. 1195–1212, Jul. 1997.